COMP 2711 Discrete Mathematical Tools for CS
Spring Semester, 2016
Written Assignment # 7
Distributed: 13 April 2016 – Due: 4pm, 20 April 2016

Your solutions should contain (i) your name, (ii) your student ID #, (ii) your email address, and (iv) your tutorial section. Your work should be submitted to the collection bin outside Room 4210 (Lift 21).

Problem 1: What is 37 mod 17? What is -4 mod 17? What is -37 mod 17? When answering these questions please also give the associated values q and r in the representation $m = qn + r$.

Problem 2: Prove the following distributive law of Modular Multiplication.
$(a +_n b) \cdot_n c = a \cdot_n c +_n b \cdot_n c$

Problem 3: Encrypt the message `COMPUTER SCIENCE` using a Caesar cipher in which each letter is shifted four places to the left.

Problem 4: A Caesar cipher with shift k letters (to the left or to the right) has been executed on some original plaintext message. The resulting ciphertext is `SZH SLCO HLD ESTD EZ OPNZOP`. What is k and what was the original message?

Problem 5: It is easy to see that 0, 5, 10, and 15 are all solutions to the equation

$$4 \cdot_{20} x = 0.$$

Are there any integral values of a and b, with $1 \leq a < 20$ and $1 \leq b < 20$, for which the equation $a \cdot_{20} x = b$ does *not* have any solutions in Z_{20}? If there are, give one set of values for a and b and explain how you know that there are no solutions to $a \cdot_{20} x = b$. If there are not, explain how you know this. (You could write out the entire Z_{20} multiplication table to justify your answer, but this is not necessary)

Problem 6: (a) Write the $\cdot_9$ multiplication table for Z_9.

(b) Which non-zero elements in Z_9 have a multiplicative inverse? Which do not?

Problem 7: Does there exist an x in Z_{147} that solves

$$12 \cdot_{147} x = 7?$$

If yes, give the value of x (it is not necessary to show your work).
If no, prove that such an x does not exist.